## B13 Forensic Analysis of Twitter® Artifacts Using the Twitter® Web Interface and TweetDeck®

*Jonathan P. Fowler, MS*, First Advantage Litigation Consulting, 1828 L St NW, Ste 1070, Washington, DC 20036; and Paul A. Taylor, MS*, First Advantage Litigation Consulting, 420 Lexington Ave, Ste 2520, New York, NY 10170*

After attending this presentation, attendees will have an understanding of types of artifacts left behind on a computer running the Windows operating system using the Twitter® web interface and using the popular TweetDeck® desktop software offered by Twitter®.

This presentation will impact the forensic science community by providing information to assist in the identification of artifacts used to determine if a suspect computer was used in the composition or review of messages using either the Twitter® web platform or the TweetDeck® desktop application. Although geared primarily toward an audience of digital forensics investigators/analysts/examiners, it is also well suited for attorneys, paralegals, or other legal professionals who often deal with evidence emanating from social media platforms, such as Twitter®.

The web interface will be tested through a variety of browsers, to include Microsoft Internet Explorer® (versions 8 and 9), Mozilla Firefox® (version 14), Apple Safari® (version 5), and Google Chrome® (version 20). The TweetDeck software will be tested by downloading and installing it on a clean installation of Windows 7. Three dummy Twitter® accounts will also be created to aid in the testing process.

Founded in 2006, Twitter® is an online social media outlet that allows its users to post micro-blogs of up to 140 characters called "tweets." The rapid growth and acceptance of Twitter® by the public is evidenced by the fact that the company now has over 500 million users; and, according to the web information site Alexa, their most recent three-month tracking numbers show that Twitter® is the eighth most popular website in the world.[1] Its social significance can also be gauged by the enormous popularity of segments on late-night talk show television programs where celebrities appear on the show to read mean-spirited tweets about themselves.

Although there currently exist multiple third-party options from which a user can access and utilize a Twitter® account (i.e., HootSuite, Tweetings, Echofon, etc.), a recent article on TechCrunch.com cites statements made by the founder of Semiocoast, a French social media monitoring company, that "Twitter's® own access points, including TweetDeck, represent 75.4% of all public tweets."[2] This statistic was used to determine the most probable methods by which Twitter® artifacts would be generated, leading to the analysis performed for this presentation.

A prime example for the need of this type of analysis can be found in a 2011 case from the U.S. District Court for the District of Colorado, *Doe vs. Hofstetter*, in which the court found that the defendant created a fake Twitter® account, impersonated the plaintiff, and "communicated with third parties using the fake Twitter® account."[3] In this particular matter, knowing the types of artifacts left by the usage of Twitter® through either the web interface or through TweetDeck could have proven beneficial to those examiners investigating the defendant's computer. Additionally, the high-profile matter involving inappropriate tweets that may or may not have been sent from former Representative Anthony Weiner's Twitter® account highlights the need for reliable research to identify what, if any, artifacts are left behind on a computer by Twitter® usage.

**References:**

1. http://www.alexa.com/siteinfo/twitter.com
2. http://techcrunch.com/2012/07/31/twitter-may-have-500m-users- but-only-170m-are-active-75-on-twitters-own-clients/
3. http://scholar.google.com/scholar_case?case=7625145628958395001 &q=%5B+facebook+OR+myspace+OR+linkedin+OR+twitter+ OR+tumblr+%5D%3B+All+courts&hl=en&as_sdt=2006&as_ylo=2012

**Twitter®, Social Media, Digital Forensics**